BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-245287
(43)Date of publication of application : 01.09.1992

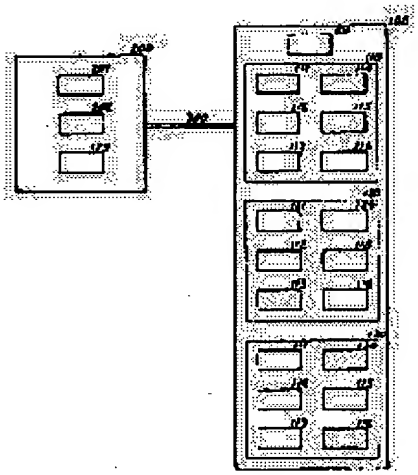
(51)Int.Cl. G09C 1/00
H04L 9/28

(21)Application number : 03-010630
(22)Date of filing : 31.01.1991

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HARADA TOSHIHARU
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(54) SECRET KEY FORMING METHOD BASED ON IDENTIFICATION INFORMATION

(57)Abstract:
PURPOSE: To form the secret key of a terminal while keeping it secret to key forming sub-centers and a key issuing center from the partial information of the secret key of the terminal and the terminal secret information held at the terminal and prevent an iniquity.
CONSTITUTION: A key forming sub-center, a sub-center information division section 112, an encoding section 113, a decoding section 114, the first arithmetic section 115, and the first arithmetic section 116 are provided to form the terminal secret key information while multiple key forming sub-centers 110, 120, 130 forming the partial information of the secret key of a terminal 200 and the terminal 200 having the terminal secret information keep the information secret respectively, a terminal information division section 201 and the encoding section 113 are provided in the terminal 200, and the second arithmetic section 202 for forming a terminal secret key from the terminal secret key information and the terminal secret information is provided in the terminal 200.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平4－245287

(43)公開日　平成４年(1992)９月１日

(51)Int.Cl.⁵	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０９Ｃ　1/00		7922－5L		
Ｈ０４Ｌ　9/28				
		7117－5K	Ｈ０４Ｌ　9／02	Ａ

審査請求　未請求　請求項の数３(全　６　頁)

(21)出願番号　特願平3－10630

(22)出願日　平成３年(1991)１月31日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

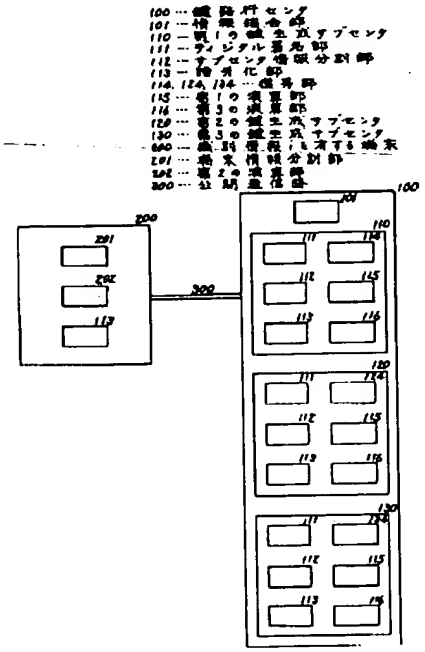
(74)代理人　弁理士　小鍛治　明　（外２名）

(54)【発明の名称】　識別情報に基づく秘密鍵生成方式

(57)【要約】

【構成】　端末の秘密鍵の部分情報を生成する複数の鍵生成サブセンタ１１０、１２０、１３０と、端末秘密情報を有する端末２００が、以上の情報をそれぞれを秘密に保ちつつ、端末秘密鍵情報を生成するために、鍵生成サブセンタにサブセンタ情報分割部１１２と暗号化部１１３と復号部１１４と第１の演算部１１５と第１の演算部１１６を設け端末に、端末情報分割部２０１と暗号化部１１３を設け、さらに端末に、その端末秘密鍵情報と端末秘密情報から端末秘密鍵を生成するため第２の演算部２０２を設ける。

【効果】　端末の秘密鍵の部分情報と、端末の保持する端末秘密情報から、端末の秘密鍵を、各鍵生成サブセンタや鍵発行センタに秘密に保ちつつ生成でき、鍵発行センタおよび鍵生成サブセンタに不正を防ぐことができる。



1

【特許請求の範囲】

【請求項1】鍵発行センタと端末とそれらを結ぶ公開通信路からなるシステムにおいて、前記鍵発行センタは、複数の鍵生成サブセンタと、複数の情報を一つの情報に結合する情報結合部を備え、前記各鍵生成サブセンタは、マスター公開鍵とそれぞれのサブセンタ秘密鍵を有し、さらに前記サブセンタ秘密鍵を用いてディジタル署名を生成するディジタル署名部と、一つの情報を複数の情報に分割するサブセンタ情報分割部と、前記各鍵生成サブセンタそれぞれに向けて情報の暗号化を行う暗号化部と、自身に向けられた暗号化された情報を復号する復号部と、第1の演算部を備え、前記端末は、マスター公開鍵と公開の端末識別情報と端末秘密情報を有し、さらに一つの情報を複数の情報に分割する端末情報分割部と、前記各鍵生成サブセンタそれぞれに向けて情報の暗号化を行う暗号化部と、第2の演算部を備え、前記端末が、前記端末秘密情報を、前記端末情報分割部に入力し、その出力として、複数の端末秘密部分情報を生成し、これらの端末秘密部分情報を、それぞれ前記暗号化部で暗号化し、その出力として暗号化された端末秘密部分情報を生成し、前記端末識別情報と、前記暗号化された端末秘密部分情報を、前記鍵発行センタに前記公開通信路を介して通知し、端末秘密鍵情報の発行を要求する端末秘密鍵情報要求ステップと、前記鍵発行センタが、前記各鍵生成サブセンタに、端末より通知された、前記端末識別情報と前記暗号化された端末秘密部分情報を通知し、端末秘密鍵部分情報の生成を依頼する端末秘密鍵部分情報生成依頼ステップと、前記各鍵生成サブセンタが、通知された前記端末識別情報を、前記ディジタル署名部に入力し、その出力として端末部分秘密鍵を求め、この端末部分秘密鍵を、前記サブセンタ情報分割部に入力し、その出力として複数の端末部分秘密鍵部分情報を生成し、これらの端末部分秘密鍵部分情報を、それぞれ、前記暗号化部で暗号化し、その出力として暗号化された端末部分秘密鍵部分情報を生成し、これらの暗号化された端末部分秘密鍵部分情報を、それぞれ前記各鍵生成サブセンタに通知し、前記各鍵生成サブセンタが、それぞれ、前記各鍵生成サブセンタより通知された前記暗号化された端末部分秘密鍵部分情報と前記鍵発行センタより通知された前記暗号化された端末秘密部分情報の中で、自信に向けられた情報を、前期復号部で復号し、その出力として、自信に向けられた前記端末部分秘密鍵部分情報と前記端末秘密部分情報を生成しこれらの端末部分秘密鍵部分情報と端末秘密部分情報を、前記第1の演算部に入力し、その出力として、端末秘密鍵部分情報を生成し、この端末秘密鍵部分情報を、前記鍵発行センタに通知する端末秘密鍵部分情報生成ステップと、前記鍵発行センタが、前記各鍵生成サブセンタからそれぞれ通知された前記端末秘密鍵部分情報を、前記情報結合部で結合し、その出力として、端末秘密鍵情報を生成し、この端末秘密鍵情報を、公開通信路を介して、前記端末に通知する端末秘密鍵情報発行ステップと、前記端末が、通知された前期端末秘密鍵情報と前記端末秘密情報を、前記第2の演算部に入力し、その出力として、端末の秘密鍵を生成する端末秘密鍵生成ステップより構成される識別情報に基づく秘密鍵生成方式。

2

【請求項2】各鍵生成サブセンタは、請求項1の構成に加えて第3の演算部を備え、新たに、マスタ鍵生成ステップを追加し、そのマスタ鍵生成ステップにおいて、前記各鍵生成サブセンタの有するサブセンタ秘密鍵を、前期サブセンタ情報分割部に入力し、その出力として、複数のサブセンタ秘密鍵部分情報を生成し、このサブセンタ秘密鍵部分情報を、それぞれ、前記暗号化部で暗号化し、その出力として、暗号化されたサブセンタ秘密鍵部分情報を生成し、これらの暗号化されたサブセンタ秘密鍵部分情報を、前記各鍵生成サブセンタに通知し、前記各鍵生成サブセンタが、前記各鍵生成サブセンタより通知された前記暗号化されたサブセンタ秘密鍵部分情報の中で、自信に向けられた情報を、前記復号部で復号し、その出力として、自信に向けられた前記サブセンタ秘密鍵部分情報を生成し、これらのサブセンタ秘密鍵部分情報を第3の演算部に入力し、その出力としてマスタ公開鍵部分情報を求め、そのマスタ公開鍵部分情報を鍵発行センタに通知し、前記鍵発行センタは、通知された前記マスタ公開鍵部分情報を、前記情報結合部に入力し、その結果をマスタ鍵とすることを特徴とする特許請求の範囲第1項記載の秘密鍵生成方式。

【請求項3】マスタ鍵生成ステップにおいて、第1のマスタ公開鍵eと、第1のサブセンタ秘密鍵として素数pjと、第2のサブセンタ秘密鍵として、(pj-1)を法とする前記eの乗法的逆数djを有する鍵生成サブセンタj（1≦j≦n）が、前記第1のサブセンタ秘密鍵pjを前期サブセンタ情報分割部に入力し、その出力として、複数のサブセンタ秘密鍵部分情報pjk（1≦k≦n）を生成し、これらのpjkを、それぞれ、前期暗号化部Ek（1≦k≦n）で、暗号化し、その出力として暗号化されたサブセンタ秘密鍵部分情報Ek(pjk)（1≦k≦n）を生成し、これらのEk(pjk)を、それぞれ前期各鍵生成サブセンタに通知し、鍵生成サブセンタk（1≦k≦n）が、前記各鍵生成サブセンタより通知された前記Ek(pjk)（1≦j≦n）を、それぞれ、前期復号部で復号し、前記サブセンタ秘密鍵部分情報pjk（1≦j≦n）を求め、このpjk（1≦j≦n）を、第3の演算部に入力し、前記pjk（1≦j≦n）の積Pkを求め、このPkをマスタ公開鍵部分情報として前記鍵発行センタに通知し、前記鍵発行センタは、通知された前記マスタ公開鍵部分情報Pk（1≦k≦n）を、前記情報結合部に入力し、その出力として第2のマスタ公開鍵Pを生成し、前期端末秘密鍵情報要求ステップで、端末秘密情報rと、識別情報iを有する端末が、前記rを前期端末情報分割部に入力し、その出力

3

として端末秘密部分情報rk（1≦k≦n）を生成し、このrkを、それぞれ、前期暗号化部Ek（1≦k≦n）で暗号化し、その出力として、暗号化された端末秘密部分情報Ek(rk)を生成し、前記端末識別情報iと前記Ek(rk)（1≦k≦n）を前記鍵発行センタに通知し、端末秘密鍵部分情報生成依頼ステップで、前記鍵発行センタが、前記各鍵生成サブセンタj（1≦j≦n）に、前記端末識別情報iと、前記暗号化された端末秘密部分情報Ej(rj)（1≦j≦n）を通知し、端末秘密鍵部分情報生成ステップで、鍵生成サブセンタj（1≦j≦n）は、前記端末識別情報iを、ディジタル署名部に入力し、その出力として、次式を満たすSj

$Sj = aj \times bj \times (i^{4}) \mod pj$

ただし　$aj = P / pj$

$bj \times aj = 1 \mod pj$

を端末部分秘密鍵として求め、このSjを、前記サブセンタ情報分割部に入力し、複数の端末部分秘密鍵部分情報Sjk（1≦k≦n）を生成し、このSjkを、前期暗号化部Ek（1≦k≦n）で、暗号化し、その出力として、前記暗号化された端末部分秘密鍵部分情報Ek(Sjk)（1≦k≦n）を生成し、このEk(Sjk)を、前記各鍵生成サブセンタに通知し、鍵生成サブセンタk（1≦k≦n）が、前記各鍵生成サブセンタより通知された前記暗号化された端末部分秘密鍵部分情報Ek(Sjk)（1≦j≦n）と前記鍵発行センタから通知された前記暗号化された端末秘密部分情報Ek(rk)を、それぞれ前記復号部で復号し、前記端末部分秘密鍵部分情報Sjk（1≦j≦n）と前記端末秘密部分情報rkを求め、このSjk（1≦j≦n）と前記rkを、第1の演算部に入力し、前記Sjk（1≦j≦n）とrkそれぞれの和Sk'を、端末秘密鍵部分情報として求め、前記Sk'を、前記鍵発行センタに通知し、端末秘密鍵情報発行ステップで、前記鍵発行センタが、前記各鍵生成サブセンタから通知された前記端末秘密鍵部分情報Sk'（1≦k≦n）を、前記情報結合部で結合して端末秘密鍵情報Sを生成し、このSを前記公開通信路を用いて前記端末に通知し、端末秘密鍵生成ステップで、前記端末が、通知された前期端末秘密鍵情報Sと前記端末秘密情報rを、前記第2の演算部に入力して、前記Sとrの差Sを端末の秘密鍵を生成することを特徴とする特許請求の範囲第2項記載の秘密鍵生成方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、識別情報に基づく暗号方式における秘密鍵の生成方式に関する。

【0002】

【従来の技術】識別情報に基づく暗号方式として、シャミアーの提案したディジタル署名方式、太田の提案した認証方式、岡本および田中の提案した暗号鍵配送方式がある。（シャミアーの方式は、"アイデンティティ　ベースト　クリプトシステム　アンド　シグネチャー　スキームズ"プロシーディング　オヴ　クリプト84　pp47-53 1984.8に、太田の方式は、"RSA暗号系を利用した個人識別情報に基づく認証方式"電子情報通信学会論文誌D-1　vol.J72-D-1　NO.8　pp612-6321989.8に、岡本及び田中の方式は、"ID情報に基づく暗号鍵配送方式の提案"電子情報通信学会論文誌D-1　vol.72-D-1　No.4　pp293-300　1989.4にそれぞれ詳しい。）これらの方式は、いずれも、信頼のおける単一の鍵発行センタが、各端末に対して、その端末固有の識別情報に対応する秘密鍵を発行する端末秘密鍵発行ステップと、各端末が、発行された秘密鍵を用いて、ディジタル署名、相手認証、あるいは、鍵共有などの暗号プロトコルを実行する暗号プロトコル実行ステップからなる。これらの方式における端末秘密鍵発行ステップは、いずれも、RSAディジタル署名法を用いて次のように実行される。（RSAディジタル署名については、"現代暗号理論"小山他著、電子情報通信学会編に詳しい。）

4

端末の秘密鍵発行ステップ

（1）鍵発行センタの初期設定

鍵発行センタは、2素数p1、p2を生成し、それらの積Pを求め、L＝LCM（p1-1、p2-1）に互いの素な数eを生成し、Lを法とする剰余環のなかで乗法的逆数dを生成し、Pは、端末に公開し、（p1、p2、d）は秘密に保持する。

（2）端末による秘密鍵発行要求

端末は、固有の識別情報iを、鍵発行センタに通知し、秘密鍵の発行を要求する。

（3）端末の秘密鍵生成

鍵発行センタは、端末の秘密鍵Siを、秘密鍵（p1、p2、d）を用いたRSAディジタル署名

$Si = i^{d} \mod P$　（ただしP＝p1×p2）

より求め、端末iに秘密に送る。ここで、（a mod b）は、aをbで割ったときの剰余を表わす。このようにして生成された秘密鍵Siを用いて、この後、各種暗号プロトコルが実行される。このような手順で端末の秘密鍵を発行する場合、鍵発行センタは任意の端末の秘密鍵を知ることができることは明かである。従って、仮にセンタが悪意を持ったとき、端末iの秘密鍵Siを鍵発行センタが悪用するすることが容易である。

【0003】

【発明が解決しようとする課題】このように、従来の方式では、単一の鍵発行センタが、ディジタル署名によって端末の秘密鍵を生成するため、その鍵発行センタは、端末の秘密鍵を容易に知ることができ、鍵発行センタによって端末の秘密鍵を悪用されかねないという問題点を有している。本発明は、上述の問題点に鑑みて試されたもので、鍵発行センタが、端末の秘密鍵を知ることのできない、識別情報に基づく秘密鍵生成法を提供することを目的とする。

【0004】

5

【課題を解決するための手段】本発明は上述の問題点を解決するため、複数の鍵生成サブセンタと情報結合部からなる鍵発行センタと、サブセンタ秘密鍵を有し、さらに、サブセンタ秘密鍵を用いるディジタル署名部とサブセンタ情報分割部と暗号化部と復号部と第１の演算部と第３の演算部からなる鍵生成サブセンタと、端末秘密情報を有し、さらに、端末情報分割部と暗号化部と第２の演算部からなる端末と公開通信路からなるという構成を備えたものである。

【０００５】

【作用】本発明は上述の構成によって、端末が、端末秘密情報を端末情報分割部で分割し、その結果を端末秘密部分情報として、各鍵生成サブセンタに秘密に通知し、鍵生成サブセンタが、端末の識別情報に対応する端末部分秘密鍵を、サブセンタ情報分割部で分割し、その結果を端末部分秘密鍵部分情報として、各鍵生成サブセンタに秘密に通知し、さらに各鍵サブセンタが、各鍵生成サブセンタから通知された端末部分秘密鍵部分情報と、端末より秘密に通知された端末秘密部分情報を第１の演算部に入力し、その出力として、端末秘密鍵部分情報を生成し、それを鍵発行センタに通知し、鍵発行センタが、その端末秘密鍵部分情報を、情報結合部で結合し、その結果として端末秘密鍵情報を生成し、それを、端末に通知し、端末が、その端末秘密鍵情報と端末秘密情報から端末の秘密鍵を生成するため、鍵発行センタおよび鍵生成サブセンタに端末の秘密鍵が知られることがなく、鍵発行センタおよび鍵生成サブセンタのセンタの不正を防ぐことができる。

【０００６】また、上述の構成によって、鍵生成サブセンタが、サブセンタ秘密鍵を、サブセンタ情報分割部で分割し、その結果としてサブセンタ秘密鍵部分情報を生成し、それを各鍵生成サブセンタに秘密に通知し、各鍵生成サブセンタが、通知されたサブセンタ秘密鍵部分情報を、第３の演算部に入力し、その出力としてマスタ公開鍵部分情報を生成し、それを鍵発行センタに通知し、鍵発行センタが、マスタ公開鍵部分情報を情報結合部で結合し、その結果として、マスタ公開鍵生成することができるため、サブセンタのサブセンタ秘密鍵を、秘密に保ちつつマスタ公開鍵を生成でき、鍵発行センタおよび鍵生成サブセンタのセンタの不正を防ぐことができる。

【０００７】

【実施例】図１は本発明の一実施例による識別情報に基づく秘密鍵生成方式の概略構成を示すものであって、１００は、端末に、端末秘密鍵情報を発行する鍵発行センタであり、２００は、識別情報Ｉを有する端末であり、３００は、公開通信路であり１００を構成する１１０、１２０、１３０は、それぞれ端末秘密鍵部分情報を生成する、第１の鍵生成サブセンタ、第２の鍵生成サブセンタ、第３の鍵生成サブセンタであり、１０１は、情報結合部であり、１１０を構成する１１１は、端末の部分秘密鍵を生成するディジタル署名部であり、１１２は、サブセンタ情報分割部であり、１１３は、第１、第２、第３の暗号化関数からなる暗号化部であり、１１４は、第１の復号関数からなる復号部であり、１１５は、加算演算を行なう１の演算部であり、１１６は、乗算演算を行なう第３の演算部であり、１２０を構成する１１１は、端末の部分秘密鍵を生成するディジタル署名部であり、１１２は、サブセンタ情報分割部であり、１１３は、第１、第２、第３の暗号化関数からなる暗号化部であり、１２４は、第２の復号関数からなる復号部であり、１１５は、加算演算を行なう１の演算部であり、１１６は、乗算演算を行なう第３の演算部であり、１３０を構成する１１１は、端末の部分秘密鍵を生成するディジタル署名部であり、１１２は、サブセンタ情報分割部であり、１１３は、第１、第２、第３の暗号化関数からなる暗号化部であり、１３４は、第３の復号関数からなる復号部であり、１１５は、加算演算を行なう１の演算部であり、１１６は、乗算演算を行なう第３の演算部であり、２００を構成する２０１は、端末秘密情報を分割する端末情報分割部であり、２０２は、減算演算を行なう第２の演算部であり、１１３は、第１、第２、第３の暗号化関数からなる暗号化部である。

6

【０００８】次に、実施例の動作について述べる。

（１）マスタ公開鍵生成ステップ

第１の鍵生成サブセンタ１１０を例に述べる、第２、第３の鍵生成サブセンタ１２０、１３０も同様に動作する。

【０００９】(1.1)サブセンタ秘密鍵部分情報の生成

第１の鍵生成サブセンタ１１０は、　第１のマスタ公開鍵として素数ｅと、第１のサブセンタ秘密鍵として素数ｐ1と、第２のサブセンタ秘密鍵として次式を満たすd1

$$e \times d1 = 1 \mod (p1-1)$$

を保持し、このｐ1を、サブセンタ分割部１１２に入力し、ｐ1の部分情報ｐ1ｋ（k=1、2、3）を生成する。なお、サブセンタ分割部１１２は、ある３個の数のそれぞれの分割値毎の積が、元の３個の数の積の分割値となる分割関数を有する。

【００１０】(1.2)サブセンタ秘密鍵部分情報の暗号化と通知

第１の鍵生成サブセンタ１１０は、ｐ1の部分情報ｐｉｋ（k=1、2、3）を、暗号化部１１３で暗号化してEk(p1k)（k=1、2、3）を求め、E1(p11)は、保持し、E2(p12)、E3(p13)は、それぞれ、第２、第３の鍵生成サブセンタに通知する。

【００１１】(1.3)サブセンタ秘密鍵部分情報の復号とマスタ公開鍵部分情報の生成

第１の鍵生成サブセンタ１１０は、通知されたE1(p11)、E1(p21)、E1(p31)を、復号部１１４で復号し、サブセンタ秘密鍵部分情報p11、p21、p31を求め、これらを第３の演算部１１６で、

7

P1'＝p11×p21×p31
を求め、マスタ公開鍵部分情報として、鍵発行センタに通知する。なお、ここでの乗算は、ある有限環上での乗算である。

【００１２】(1.4)マスタ公開鍵の生成
鍵発行センタは、通知されたP1'、P2'、P3'を情報結合部に入力し
P＝P1'×P2'×P3'　(＝p1×p2×p3)
を求める。なお、ここでの乗算は、ある有限環上での乗算である。なお、情報結合部は、サブセンタ分割部の分割関数の逆関数を有する。

【００１３】以上のステップにより、サブセンタ秘密鍵p1、p2、p3を秘密に保ちつつ、その積を求めることが可能である。

（２）端末秘密鍵情報要求ステップ
(2.1)端末秘密部分情報の生成
識別情報ｉを有する端末２００は、端末秘密情報としてある乱数値ｒを保持し、このｒを、端末分割部２０１に入力し、端末秘密部分情報ｒk（k=123）を生成する。なお、端末分割部２０１は、ある３個の数のそれぞれの分割値毎の和が、元の３個の数の和の分割値となる関数を有する。

【００１４】(2.2)端末秘密部分情報の暗号化と端末秘密鍵情報の要求
端末２００は、端末秘密部分情報ｒk（k=1、2、3）を、暗号化部１１３で暗号化し、Ek(ｒk)（k=1、2、3）を求め、識別情報ｉおよびE1(ｒ1)、E2(ｒ2)、E3(ｒ3)を、それぞれ鍵発行センタに通知する。

（３）端末秘密鍵部分情報生成依頼ステップ
端末から通知された識別情報ｉおよびE1(ｒ1)、E2(ｒ2)、E3(ｒ3)を、それぞれ鍵生成サブセンタに通知する。

（４）端末秘密鍵部分情報生成ステップ
第1の鍵生成サブセンタ１１０を例に述べる、第2、第3の鍵生成サブセンタ１２０、１３０も同様に動作する。

【００１５】(4.1)端末部分秘密鍵の生成
第１の鍵生成サブセンタは、前記端末識別情報ｉを、ディジタル署名部１１１に入力し、端末部分秘密鍵S1
S1＝a1×b1×（i^{a1}　mod　p1）
ただし　a1＝P／p1＝p1×p2
b1×a1＝1　mod　p1
を生成する。なお、ここでの乗算は、ある有限環上での乗算である。

【００１６】(4.2)端末部分秘密鍵部分情報の生成
端末部分秘密鍵S1を、サブセンタ情報分割部１１２に入力し、端末部分秘密鍵部分情報S11、S12、S13を生成する。なお、サブセンタ末分割部２０１は、ある３個の数のそれぞれの分割値毎の和が、元の３個の数の和の分割値となる関数を有する。

8

【００１７】(4.2)端末部分秘密鍵部分情報の暗号化と通知
端末部分秘密鍵部分情報S11、S12、S13を、暗号化部１１３で、暗号化し、E1(S11)、E2(S12)、E3(S13)を生成しE1(S11)、E2(S12)、E3(S13)を、各鍵生成サブセンタに通知する。

【００１８】(4.3)端末部分秘密鍵部分情報の復号
各鍵生成サブセンタより通知された暗号化された端末部分秘密鍵部分情報E1(S11)、E1(S21)、E1(S31)と、前記鍵発行センタから通知された暗号化された端末秘密部分情報E1(r1)を、それぞれ復号部１１４で復号し、端末部分秘密鍵部分情報S11、S21、S31と、端末秘密部分情報r1を生成する。

【００１９】(4.4)端末秘密鍵部分情報の生成
端末部分秘密鍵部分情報S11、S21、S31と、端末秘密部分情報r1を第１の演算部１１５に入力して、その出力として、端末秘密鍵部分情報S1S1＝S11＋S21＋S31＋r1を生成し、鍵発行センタに通知する。なお、ここでの加算は、ある有限環上での加算である。

（５）端末秘密鍵情報発行ステップ
鍵発行センタが、各鍵生成サブセンタから通知された端末秘密鍵部分情報S1'、S2、S3を、情報結合部１０１で結合して、端末秘密鍵情報Sを生成し、このSを公開通信路３００を介して、端末２００に発行する。なお、情報結合部は、サブセンタ分割部および端末の分割部の分割関数の逆関数を有する。

（６）端末秘密鍵生成ステップ
端末が、通知された端末秘密鍵情報Sと端末秘密情報ｒを、第２の演算部２０２に入力し、その出力として、端末の秘密鍵Ｓ
Ｓ＝S－ｒ
を生成する。なお、ここでの減算は、ある有限環上での減算である。以上のステップにより、鍵生成サブセンタの生成した端末の部分秘密鍵S1、S2、S3、および、端末秘密情報ｒを秘密に保ちつつ、秘密鍵Ｓを求めることが可能である。

【００２０】すなわち各鍵生成サブセンタは、生成した端末部分秘密鍵を、端末や他の鍵生成サブセンタや鍵発行センタに秘密に保ちつつ、また、端末は、端末の端末秘密情報を、各鍵生成サブセンタや鍵発行センタに秘密に保ちつつ、端末部分秘密鍵と端末秘密情報から端末秘密鍵情報が生成され、端末によって、その端末秘密鍵情報と端末秘密情報より端末の秘密鍵をが生成できるため、鍵発行センタおよび鍵生成サブセンタに端末の秘密鍵が知られることがなく、鍵発行センタの不正を防ぐことができる。

【００２１】
【発明の効果】以上の説明から明らかなように、本発明は、鍵発行センタが端末の部分秘密鍵を生成する鍵生成サブセンタを複数備え、各鍵生成サブセンタが、端末よ

9

り秘密に通知された端末秘密部分情報と、各鍵生成サブセンタより秘密に通知された端末部分秘密鍵部分情報を、第１の演算部に入力して端末秘密鍵部分情報を求め、鍵発行センタが、情報結合部でその端末秘密鍵部分情報結合して端末秘密鍵情報を生成し、端末が、その端末秘密鍵情報と端末秘密情報から端末秘密鍵を生成するという構成を備えることにより、各鍵生成センタ秘密情報である端末部分秘密鍵と端末の秘密情報である端末秘密情報を、秘密に保ちつつ、端末によって、端末の秘密鍵が生成できるため、鍵発行センタおよび鍵生成サブセンタに端末の秘密鍵が知られることがなく、鍵発行センタの不正を防ぐことができる。

【図面の簡単な説明】

【図１】本発明の実施例の構成図である。

【符号の説明】

１００　鍵発行センタ

10

２００　識別情報ｉを有する端末
３００　公開通信路
１０１　情報結合部
１１０　第１の鍵生成サブセンタ
１１１　ディジタル署名部
１１２　サブセンタ情報分割部
１１３　暗号化部
１１４　復号部
１１５　第１の演算部
１１６　第３の演算部
１２０　第２の鍵生成サブセンタ
１２４　復号部
１３０　第３の鍵生成サブセンタ
１３４　復号部
２０１　端末情報分割部
２０２　第２の演算部

【図１】